

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

COMMUNICATION OF
INTERNATIONAL APPLICATIONS

(PCT Article 20)

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C. 20231
ETATS-UNIS D'AMERIQUE

Date of mailing:

03 April 2000 (03.04.00)

in its capacity as designated Office

The International Bureau transmits herewith copies of the international applications having the following international application numbers and international publication numbers:

International application no.:

PCT/JP99/04328

International publication no.:The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

E P



P C T

国際調査報告

(法 8 条、法施行規則第40、41条)
〔PCT 18 条、PCT 規則43、44〕

出願人又は代理人 の書類記号 99-F-037PCT	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/J P 99/04336	国際出願日 (日.月.年) 11.08.99	優先日 (日.月.年) 12.08.98
出願人(氏名又は名称) 森永乳業株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT 18 条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT 規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 _____ 図とする。 ☐ 出願人が示したとおりである。

☒ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁶ A61K31/66, 31/195, 38/01, 38/16, 38/40,
35/78, 31/23, 31/20, 31/70, 33/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁶ A61K31/66, 31/195, 38/01, 38/16, 38/40,
35/78, 31/23, 31/20, 31/70, 33/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)
CAPLUS (STN)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 1-128919, A (雪印乳業株式会社) 1. 5月. 1989 (22. 05. 89) 全文 (ファミリーなし)	1-3

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

05. 11. 99

国際調査報告の発送日

16.11.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA / JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

森井 隆信

4C

9841

電話番号 03-3581-1101 内線 6460



PCT

国際調査報告

(法8条、法施行規則第40、41条)

[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 PCT001JST	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/J P 99/04328	国際出願日 (日.月.年) 10.08.99	優先日 (日.月.年) 24.09.98
出願人(氏名又は名称) 平野 琢也		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁸ H04L9/38, H04B10/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁸ H04L9/38, H04B10/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996
 日本国公開実用新案公報 1971-1999
 日本国登録実用新案公報 1994-1999
 日本国実用新案登録公報 1996-1999

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	M. J. Werner, G. J. Milburn; "Eavesdropping using quantum-nondemolition measurements", PHYSICAL REVIEW A, Vol. 47, No. 1 (1993) p. 634-641	1, 5, 8-11
Y A		12-14 2-4, 6, 7
Y	H. Bartelt, K. -H. Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics", ISRAEL Journal of TECHNOLOGY, Vol. 18, No. 5 (1980) p. 260-262	12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

02.11.99

国際調査報告の発送日

16.11.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

4229

電話番号 03-3581-1101 内線 3576

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	副島俊雄, 貝淵俊二 著; 新版・光ファイバ通信 株式会社電気通信技術ニュース社 発行, (12. 12. 1981) p. 252-253	13, 14
A	C. Marand, P. D. Townsend; "Quantum key distribution over distances as long as 30km.", Optics Letter, Vol. 20, No. 12 (1995) p. 1695-1697	1-14
A	Yi Mu, Yuliang Zheng, Yan-Xia Lin; "Multi-User Quantum Cryptography", International Symposium on Information Theory & Its Application 1994, Vol. 1 (1994) p. 245-250	1-14
A	B. A. Slutsky, R. Rao, P. -C. Run, Y. Fainman; "Security of cryptography against individual attacks", PHYSICAL REVIEW A, Vol. 57, No. 4 (1998) p. 2383-2390	1-14
A	松枝秀明; "量子暗号の現状と期待", 電子情報通信学会誌, Vol. 81, No. 3 (25. 03. 1998) p. 225-228	1-14

27
000
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PCT001JST	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/JP99/04328	International filing date (day/month/year) 10 August 1999 (10.08.99)	Priority date (day/month/year) 24 September 1998 (24.09.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/38, H04B 10/00		
Applicant HIRANO, Takuya		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of <u>4</u> sheets, including this cover sheet. <input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of _____ sheets.
3. This report contains indications relating to the following items: I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input type="checkbox"/> Certain observations on the international application

Date of submission of the demand 10 August 1999 (10.08.99)	Date of completion of this report 20 April 2000 (20.04.2000)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP99/04328

I. Basis of the report

1. With regard to the elements of the international application:*

- ☒ the international application as originally filed
- ☐ the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP99/04328

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	2-4,6,7,12-14	YES
	Claims	1,5,8-11	NO
Inventive step (IS)	Claims	2-4,6,7	YES
	Claims	1,5,8-14	NO
Industrial applicability (IA)	Claims	1-14	YES
	Claims		NO

2. Citations and explanations

Claims 1, 5, 8 through 11

Document 1 (Werner, M.J., G.J. Milburn, "Eavesdropping using quantum-nondemolition measurements," PHYSICAL REVIEW A, Vol. 47, No. 1 (1993), p. 639-641) describes, in quantum cryptocommunication using optical signals, art for detecting eavesdropping based on the quantum mechanical probability distribution of the difference signal of the signal light. The inventions described in claims 1, 5, and 8 through 11 constitute a portion of the art described in document 1, and thus do not appear to possess novelty.

Claim 12

Document 2 (Bartelt, H., Brenner, K.H., "The Wigner Distribution Function: An Alternate Signal Representation in Optics," Israel Journal of Technology, Vol. 18, No. 5, p. 260-262) describes art using the Wigner distribution function as a method of representation in optical telecommunications. It would be obvious for a party skilled in the art to use the optical signal representation method of the Wigner distribution function described in document 2 as the representation method of the probability distribution of the difference signal of the signal light described in document 1.

Claims 13, 14

Document (Fukushima, S., Kaibuchi, S., "Shinpan: Tsuu-fibaa Tsuushin," Kabushiki Kaisha Denkitsushin Gijutsu Nyuusu Sha (12 December 1981), p. 252-3) states that when such photo diodes as photo diodes made of silicon (Si) and photo diodes made of InGaAs are used as an element to convert optical signals into electricity, the transmission wavelength is 0.8 to 0.9 μm when a silicon photo diode is used, and is 1.1 to 1.7 μm when an InGaAs photo diode is used. It would be obvious to a party skilled in the art to use a photo diode made from the respective materials corresponding to the respective wavelengths as described in document 3 as the signal light receiving optical element for optical telecommunications described in document 1.

Claims 2 through 4, 6 and 7

Document 4 (Marand, C., Townsend, P.D., "Quantum key distribution over distances as long as 30 km.," Optics Letters, Vol. 20, No. 12 (1995), p. 1695-1697) is a document indicating the general state of the art in the relevant technical field. It describes art for the stable transmission of a cipher key using an interference measurement quantum cryptography scheme. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunication system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 4 (Yi Mu, Yuliang Zheng, Yan-Xia Lin, "Multi-User Quantum Cryptography," International Symposium on Information Theory & Its Application," Vol. 1. (1994), p. 245-250) is a document indicating the general state of the art in the relevant technical field. It describes the detection within a prescribed sphere of correlation with information of eavesdropping by interrupt/resend against a cipher common key transmission protocol based on the

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of Box V (Citations and explanations):

uncertainty principle of quantum mechanics. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunication system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 5 (Slutsky, B.A., Rao, R., Run, P.C., Fainman, Y., "Security of quantum cryptography against individual attacks." PHYSICAL REVIEW A, Vol. 57, No. 4 (1998), p. 2383-2398) is a document indicating the general state of the art in the relevant technical field. It describes (1) examination in two-condition or four-condition quantum cryptography protocol of the relationship between transmission error and the maximum volume of information that an eavesdropper is capable of extracting and (2) how said quantum cryptography protocol defends against all attacks when the optimal eavesdropping method in each case is made clear and the eavesdropping strategy is restricted so that each bit of the quantum transmission can be attacked individually. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunication system wherein optical signals are separated into intense reference signals and weak transmission signals.

Document 6 (Matsugi, S., "Ryoushi angou no genjou to kitai," Denshi Jouhou Tsuushin Gakkai Shi, Vol. 81, No.3 (25.03.1998), P. 225-228) is a document indicating the general state of the art in the relevant technical field. It describes quantum cryptography capable of detecting the eavesdropping of ciphers using the exclusivity of a conjugate pair, by using a pair of conjugate physical amount and quantum cryptography that uses natural emissions to control the natural emission of optical particles by adjusting the size and material of cavities. However, none of documents 1 through 6 describe or suggest art relating to a quantum cryptocommunication system wherein optical signals are separated into intense reference signals and weak transmission signals.

PCT

国際予備審査報告

(法第12条、法施行規則第56条)
[PCT36条及びPCT規則70]

REC'D 08 MAY 2000

IPO

PCT

出願人又は代理人 の書類記号 PCT001JST	今後の手続きについては、国際予備審査報告の送付通知（様式PCT/ IPEA/416）を参照すること。	
国際出願番号 PCT/J P 99/04328	国際出願日 (日.月.年) 10.08.99	優先日 (日.月.年) 24.09.98
国際特許分類 (IPC) Int. Cl ¹ H04L9/38, H04B10/00		
出願人 (氏名又は名称) 平野 琢也		

1. 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条 (PCT36条) の規定に従い送付する。
2. この国際予備審査報告は、この表紙を含めて全部で 4 ページからなる。
- ☐ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。
(PCT規則70.16及びPCT実施細則第607号参照)
この附属書類は、全部で ページである。
3. この国際予備審査報告は、次の内容を含む。
- I ☒ 国際予備審査報告の基礎
- II ☐ 優先権
- III ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- IV ☐ 発明の単一性の欠如
- V ☒ PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- VI ☐ ある種の引用文献
- VII ☐ 国際出願の不備
- VIII ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日 10.08.99	国際予備審査報告を作成した日 20.04.00	
名称及びあて先 日本国特許庁 (IPEA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 青木 重徳	5W 4229
	電話番号 03-3581-1101 内線 3574	

I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT14条)の規定に基づく命令に
 応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。
 PCT規則70.16, 70.17)

☒ 出願時の国際出願書類

- | | | |
|-------------------------------------|----------------|----------------------|
| <input type="checkbox"/> 明細書 | 第 _____ ページ、 | 出願時に提出されたもの |
| <input type="checkbox"/> 明細書 | 第 _____ ページ、 | 国際予備審査の請求書と共に提出されたもの |
| <input type="checkbox"/> 明細書 | 第 _____ ページ、 | 付の書簡と共に提出されたもの |
| <input type="checkbox"/> 請求の範囲 | 第 _____ 項、 | 出願時に提出されたもの |
| <input type="checkbox"/> 請求の範囲 | 第 _____ 項、 | PCT19条の規定に基づき補正されたもの |
| <input type="checkbox"/> 請求の範囲 | 第 _____ 項、 | 国際予備審査の請求書と共に提出されたもの |
| <input type="checkbox"/> 請求の範囲 | 第 _____ 項、 | 付の書簡と共に提出されたもの |
| <input type="checkbox"/> 図面 | 第 _____ ページ/図、 | 出願時に提出されたもの |
| <input type="checkbox"/> 図面 | 第 _____ ページ/図、 | 国際予備審査の請求書と共に提出されたもの |
| <input type="checkbox"/> 図面 | 第 _____ ページ/図、 | 付の書簡と共に提出されたもの |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ ページ、 | 出願時に提出されたもの |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ ページ、 | 国際予備審査の請求書と共に提出されたもの |
| <input type="checkbox"/> 明細書の配列表の部分 | 第 _____ ページ、 | 付の書簡と共に提出されたもの |

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である _____ 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語
☐ PCT規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 図面の第 _____ ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

1. 見解

新規性(N)	請求の範囲	2-4, 6, 7, 12-14	有
	請求の範囲	1, 5, 8-11	無
進歩性(IS)	請求の範囲	2-4, 6, 7	有
	請求の範囲	1, 5, 8-14	無
産業上の利用可能性(IA)	請求の範囲	1-14	有
	請求の範囲		無

2. 文献及び説明(PCT規則70.7)

請求の範囲1, 5, 8-11

文献1: M. J. Werner, G. J. Milburn; "Eavesdropping using quantum-nondemolition measurements",
PHYSICAL REVIEW A, Vol. 47, No. 1 (1993) p. 639-641

には、光信号を用いる量子暗号通信において、信号光の差信号における量子力学的な確率分布の変化に基づいて盗聴を検出する技術が記載されており、請求の範囲1, 5, 8-11に記載された発明は、上記文献1に記載された技術の一部をなすものであり、新規性を有しない。

請求の範囲12

文献2: H. Bartelt, K.-H. Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics",
ISRAEL Journal of TECHNOLOGY, Vol. 18, No. 5 (1980) p. 260-262

には、光通信における信号の表現方法としてウィグナー分布関数を用いる技術が記載されており、文献1に記載されている信号光の差信号における確率分布の表現方法として、文献2に記載されているウィグナー分布関数による光信号の表現方法を用いることは、当技術分野の専門家にとっては自明である。

請求の範囲13, 14

文献3: 副島俊雄, 貝淵俊二 著; 新版・光ファイバ通信
株式会社電気通信技術ニュース社 発行, (12. 12. 1981)
p. 252-253

には、光信号を電気に変換する素子としてシリコン(Si)を材料としたフォトダイオードやInGaAsを材料としたフォトダイオードが用いられ、その伝送波長はシリコンフォトダイオードを用いた場合は0.8-0.9 μ m、InGaAsフォトダイオードを用いた場合は1.1-1.7 μ mである旨が記載されており、文献1に記載されている光通信の信号光受光素子として文献2に記載されている各波長に対応した各材料からなるフォトダイオードを用いることは、当技術分野の専門家にとっては自明のものである。

補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

第 V. 2 欄の続き

請求の範囲 2 - 4, 6, 7

文献 3 : C. Marand, P. D. Townsend; "Quantum key distribution over distances as long as 30km.",
Optics Letter, Vol. 20, No. 12 (1995) p. 1695-1697

は、当該技術分野における一般的技術水準を示す文献であって、干渉測定量子暗号スキームを用いる暗号キーの安全な伝送技術が記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献 1 - 6 のいずれにも記載も示唆もされていない。

文献 4 : Yi Mu, Yuliang Zheng, Yan-Xia Lin; "Multi-User Quantum Cryptography",
International Symposium on Information Theory
& Its Application 1994, Vol. 1 (1994) p. 245-250

は、当該技術分野における一般的技術水準を示す文献であって、量子物理学の不確定性原理に基づく暗号共通鍵配送プロトコルに対して、割込/再送による盗聴が情報と相関の定式化範囲内で検出できることが記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献 1 - 6 のいずれにも記載も示唆もされていない。

文献 5 : B. A. Slutsky, R. Rao, P. -C. Run, Y. Fainman;
"Security of quantum cryptography against individual attacks",
PHYSICAL REVIEW A, Vol. 57, No. 4 (1998) p. 2383-2398

は、当該技術分野における一般的技術水準を示す文献であって、伝送誤りと盗聴者が引き出しうる最大情報量の関係を二状態及び四状態の量子暗号プロトコルにて検討するとともに、各場合における最適盗聴法を明示し、盗聴戦略を量子伝送の各ビットが個別独立的に攻撃されるように限定した場合、前記量子暗号プロトコルは全ての攻撃に対抗できることが記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献 1 - 6 のいずれにも記載も示唆もされていない。

文献 6 : 松枝秀明; "量子暗号の現状と期待",
電子情報通信学会誌,
Vol. 81, No. 3 (25. 03. 1998) p. 225-228

は、当該技術分野における一般的技術水準を示す文献であって、物理量の共役な組を用い、共役な組の排他性を利用して暗号の盗聴を検知可能とする量子暗号と、キャビティのサイズや媒質を調整することにより光子の自然放出を制御することで、自然放出を利用した量子暗号が記載されているが、光信号を強度の強い参照信号と微弱な伝送信号とに分離する量子暗号通信システムに関しては、文献 1 - 6 のいずれにも記載も示唆もされていない。

記録原本

1/3

特許協力条約に基づく国際出願願書

PCT001JST

原本(出願用) - 印刷日時 1999年08月10日 (10.08.1999) 火曜日 14時08分18秒

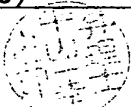
0 0-1	受理官庁記入欄 国際出願番号	PCT/JP 99/04328
0-2	国際出願日	10.08.99
0-3	(受付印)	PCT International Application 日本国特許庁
0-4 0-4-1	この特許協力条約に基づく国際出願願書(様式 - PCT/RO/101)は、右記によって作成された。	PCT-EASY Version 2.83 (updated 01.03.1999)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	PCT001JST
I	発明の名称	量子暗号通信システム
II II-1 II-2 II-4ja II-4en II-5ja II-5en II-6 II-7 II-8 II-9 II-10	出願人 この欄に記載した者は 右の指定国についての出願人である。 氏名(姓名) Name (LAST, First) あて名: Address: 国籍(国名) 住所(国名) 電話番号 ファクシミリ番号 電子メール	出願人及び発明者である (applicant and inventor) すべての指定国 (all designated States) 平野 琢也 HIRANO, Takuya 169-0075 日本国 東京都 新宿区高田馬場 2-1-1-1403 2-1-1-1403, Takadanobaba, Shinjuku-ku, Tokyo 169-0075 Japan 日本国 JP 日本国 JP 03-3232-0950 03-3232-0950 takuya.hirano@gakushuin.ac.jp

IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	平山 一幸
IV-1-1en	Name (LAST, First)	HIRAYAMA, Kazuyuki
IV-1-2ja	あて名:	160-0004 日本国 東京都 新宿区四谷 4-3-2-8
IV-1-2en	Address:	YKBサニービル 6階 YKB-Sunny Bldg. 6F 32-8, Yotsuya 4-chome, Shinjuku-ku, Tokyo 160-0004 Japan
IV-1-3	電話番号	03-3352-1808
IV-1-4	ファクシミリ番号	03-3352-2150
IV-1-5	電子メール	PED01452@nifty.ne.jp
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	--
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	US
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	
V-6	指定の確認から除かれる国	なし (NONE)
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	先の出願日	1998年09月24日 (24.09.1998)
VI-1-2	先の出願番号	平成 10 年特許願第 2 7 0 1 4 9 号
VI-1-3	国名	日本国 JP
VI-2	優先権証明書送付の請求 上記の先の出願のうち、右記の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁に対して請求している。	VI-1
VII-1	特定された国際調査機関 (ISA)	日本国特許庁 (ISA/JP)

特許協力条約に基づく国際出願願書

PCT001JST

原本（出願用） - 印刷日時 1999年08月10日（10.08.1999）火曜日 14時08分18秒

VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	3	-
VIII-2	明細書	14	-
VIII-3	請求の範囲	3	-
VIII-4	要約	1	pct001jst.txt
VIII-5	図面	7	-
VIII-7	合計	28	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	優先権書類送付請求書	-
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-17	その他	国際事務局の口座への振込を証明する書面	-
VIII-18	要約書とともに提示する図の番号	1	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)		

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	10.08.99
10-2	図面:	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であつてその後期間内に提出されたものの実際の受理の日 (訂正日)	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	23 AUGUST 1999	(23. 08. 99)
------	-----------	----------------	----------------

明 細 書

量子暗号通信システム

技術分野

この発明は、通信の安全性を確保するための秘密鍵の配布に利用され、特に伝送信号の量子力学的な状態を測定し、実質的に高い量子効率で伝送信号の検出をするための量子暗号通信システムに関する。

背景技術

通信の安全性を確保するための従来の暗号技術には、正規の通信者のみが知っている共通の秘密鍵を用いる秘密鍵暗号方式と、秘密鍵と公開鍵という一対の鍵を用いる公開鍵暗号方式とがある。

公開鍵暗号方式の暗号は、その秘蔵性を、例えば非常に大きな整数の因数分解が計算困難であるといったことに拠っているが、計算機の性能の進歩やネットワークを使った分散処理技術の発達等によりその安全性は必ずしも万全とはいえない。

これに対して、正規の通信者のみが知っている秘密鍵を送り手と受け手のみで共有することができれば絶対的に安全な通信が可能になる。このような中で、最近、秘密鍵の配布方法の秘蔵性を量子力学の原理にもとめる通信方法である量子暗号が提案されている（J. Cryptology、5、3-28（1992）C. H. Bennett et al）。

量子力学の原理によれば、測定行為は必然的に被測定対象に擾乱を与えるので、盗聴者による盗聴の試みは必ず信号に変化を与える。

したがって、信号の変化を監視することにより盗聴者の存在を暴くことができる。つまり、量子暗号を用いると距離的に離れた2点間で秘蔵性の非常に高い秘密鍵を共有することができる。従来の量子暗号は伝送信号の担い手として光を用い、かつ、光の検出に光子計数法を用いている。光子計数法とは1個以上の光子が検出器に入射したとき、ある確率（量子効率という）で電気パルスが発生する

光の検出方法である。

しかしながら、このような従来の方法では、光の検出に光子計数法を用いているため、そのことに起因する原理的及び技術的な解決すべき課題がある。

まず、原理的な課題は、伝送された後の信号の量子力学的な状態を調べることが出来ないので、盗聴者が量子非破壊測定等の高度な手段をとった場合、それを検知することができない。すなわち、盗聴者が光子数の情報を信号の光子数に変化を与えずに読み出すことが可能なので（測定の影響は位相の変化に現れる）、伝送後の光子数のみを測定していても盗聴に気がつかないことになる。

さらに技術的な課題として、光通信で通常用いられる $1.3\ \mu\text{m}$ や $1.5\ \mu\text{m}$ の光に対して、高い量子効率を有する検出器が現存しないことがある。検出の際の損失はデータの転送レートを低下させるだけでなく、原理的には盗聴者による盗聴の試みと区別できない。

そこで、この発明は、伝送信号の量子力学的な状態の測定が可能になるとともに、実質的に高い量子効率で伝送信号の検出が可能な量子暗号通信システムを提供することを目的とする。

発明の開示

この目的を達成するために、本発明の量子暗号通信システムは、光信号を用いる量子暗号通信において、盗聴の操作によって生じる信号光の差信号における振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする。

このような構成により、伝送信号の量子状態をモニターすることによって従来は困難であった量子非破壊測定のような高度な盗聴を検出することができる。

また本発明の量子暗号通信システムは、量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号と伝送信号とに位相差を付与し、これら2つの信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある2つの出力光の差を求め、伝送信号の量子状態の揺らぎに依存した出力光の差の頻度分布に基づいて送信側と受信側との秘密鍵を共有するとともに、伝送信号の量子状態の揺ら

ぎを直接測定することを特徴とするものである。

このような構成によって、参照信号の強度が強いことにより、理論的な上限に近い効率で伝送信号を検出することができる。

また本発明の量子暗号通信システムは、光源からの光を伝送信号と参照信号とに分割する第1のビームスプリッターと、伝送信号に位相変調を与える位相変調手段と、伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、参照信号に位相変調を与える位相変調手段とを備え、位相変調した微弱な伝送信号と位相変調した強度の強い参照信号とを重ね合わせて出力する第2のビームスプリッターと、第2のビームスプリッターの2つの出力光を電気変換する第1及び第2の光電変換素子と、第1及び第2の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

このような構成により、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号と伝送信号とに位相差を付与し、これら2つの信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある2つの出力の差を求め、伝送信号の量子状態の揺らぎに依存した出力の差の頻度分布に基づいて送信側と受信側の秘密鍵を共有し、伝送信号の量子状態の揺らぎを測定する。したがって、高効率の検出ができるとともに信号光の量子状態を測定することができる。

この発明は、好ましくは、上記位相変調手段が入射する光の波長程度の微小な距離を移動可能にした鏡を含んでなる。このような構成により位相変調を容易にすることができる。

また、本発明の量子暗号通信システムは、好ましくは、参照信号と伝送信号とを時間及び偏光状態で分離して同一の経路を伝送している。このような構成により、伝送路として1本の光ファイバーで伝送するので、長距離の量子暗号通信システムを提供することができる。

さらに本発明の量子暗号通信システムは、光源からの光を伝送信号と参照信号とに分割する第1のビームスプリッターと、伝送信号を一方の長い経路を通し偏光する第1の偏光素子と、伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、伝送信号に所定の位相変調を与える第1の位相変調手段と、

他方の短い経路に通した強度の強い参照信号と伝送信号とを同一光軸上に戻す第1の偏光ビームスプリッターとを備え、一本の光ファイバーを伝送してきた伝送信号及び参照信号を分離する第2の偏光ビームスプリッターと、分離した伝送信号を一方の短い経路に通し位相変調を与える第2の位相変調手段と、分離した参照信号を他方の長い経路に通し偏光する第2の偏光素子とを有しており、時間及び偏光状態が一致した伝送信号と参照信号とを重ね合わせて出力する第2のビームスプリッターと、第2のビームスプリッターの2つの出力光を電気変換する第1及び第2の光電変換素子と、第1及び第2の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

このような構成により、伝送信号と参照信号とが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、長距離の量子暗号伝送であっても2つの光の相対的な光路差の変動を小さくすることができる。

本発明の量子暗号通信システムは、好ましくは、前記光ファイバーの出力側に参照信号の偏光の乱れを補正する第3の偏光素子が設けられる。

このような構成により、光ファイバー伝送中の偏光の乱れを強度の強い参照信号で行うので、偏光の乱れを効果的に補正することができる。

さらに本発明の量子暗号通信システムは、好ましくは、出力光の差の信号に正負それぞれにしきい値を設定し、このしきい値を基準にして伝送信号の状態を判別するように構成される。

このような構成によって、しきい値を設定することにより、伝送信号の強度に応じて実効的な検出効率と誤り率とを自由に選ぶことができる。

また発明の量子暗号通信システムは、好ましくは、秘密鍵伝送のための位相変調の他に後から値の定まる位相変調を与えることによって外的な要因による参照信号と伝送信号との光路差の変動を補正するようにしている。

このような構成によって、秘密鍵伝送のための位相変調と後から定まる位相変調を与えることにより、光路差の変動の補正と量子状態の測定とを量子暗号と同時に行うことができる。

また本発明では、位相差が単調に増加する位相変調とランダムな位相変調とを

繰り返すことを特徴とする。このような構成により、光路差の変動の補正と量子状態の測定を同時に行うことができる。

またこの発明では、差信号の誤り率の増加に基づいて盗聴を検出することを特徴とする。このような構成により、盗聴の不適切な位相変調を行う確率の増加に基づき秘密鍵の誤り率が増加するため、盗聴の存在を検出することができる。

さらにこの発明では、差信号の量子力学的な状態を示すウィグナー分布関数の変化に基づいて盗聴を検出することを特徴とする。このような構成により、伝送信号の一部を分離して盗聴しても増幅過程が量子揺らぎを必ず伴うのでウィグナー分布関数の変化が生じる。したがって、ウィグナー分布関数の変化から盗聴を検出することができる。

また、本発明の量子暗号通信システムは、2つの出力光をフォトダイオードで電気変換することを特徴とする。このような構成により、高い量子効率でかつ十分なS/N比で信号の測定ができる。

さらに本発明の量子暗号通信システムは、光の波長が600nm～900nmのときシリコンフォトダイオードを用い、光の波長が1000nm～1500nmのときInGaAsフォトダイオードを用いることを特徴とする。このような構成により、高い量子効率と十分なS/N比で信号の測定ができる。

図面の簡単な説明

この発明は、以下の詳細な説明及び本発明の好ましい実施形態を示す添付図面により、より良く理解されるものとなろう。なお、添付図面に示す実施形態は本発明を特定又は限定することを意図するものではなく、単に本発明の説明及び理解を容易にするためのものである。

図中、

図1はこの発明の量子暗号通信システムの第1の実施形態の模式図である。

図2はこの発明の量子暗号通信システムにおける信号光の量子状態の揺らぎを考慮しない場合の受信者側の測定信号の模式図であり、(a)は参照光と信号光の経路の相対的な光路差とフォトダイオードに入射する光子数との関係図で、挿入図は光路差がゼロ付近の拡大図である。図2(b)は参照光と信号光との差信

号を示す図である。

図3はこの発明における信号光の量子状態の揺らぎを考慮した場合の受信者側の測定信号の模式図で、(a)は光路差が0度の場合、(b)は光路差が90度($\lambda/4$)の場合、(c)は光路差が180度($\lambda/2$)の場合、(d)は光路差が270度($3\lambda/4$)の場合であり、それぞれ横軸は差信号の大きさを示し、縦軸はその信号が検出される確率を示す。

図4は第1の実施形態の測定結果の例であり、(a)は5000回測定したときの差信号の頻度分布図で、横軸は実際の測定電圧である。(b)は(a)のような測定を30回行って得たデータから計算機トモグラフィーにより求めた信号光のウィグナー分布関数の図である。

図5はこの発明による量子暗号の手順を示す図であり、左欄の1は送信者の位相変調、2は受信者の位相変調、3は送信者と受信者の位相変調の合計、4は受信者の測定結果、5は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、0度又は180度のとき○を、90度又は270度のとき×を受信者に通知したこと、6は受信者が+にビット1を、-にビット0を、○になった場合につき当てはめ秘密鍵としたこと、7は送信者が自分の位相変調が、0度又は90度のときはビット1を、180度又は270度のときはビット0を当てはめ秘密鍵としたことを示す。

図6はこの発明の第2の実施形態の量子暗号装置の模式図である。

図7は第2の実施形態に位相変調を与える手順を示す表である。

発明を実施するための最良の形態

以下、図面に示した好適な実施形態に基づいて本発明を詳細に説明する。なお以下の説明では、本発明の例示的な実施形態について説明しているが、開示した実施形態に関して、本発明の要旨及び範囲を逸脱することなく、種々の変更、省略、追加が可能であることは当業者において自明である。したがって本発明は実施形態に限定されるものではなく、請求の範囲に記載された要素によって規定される範囲及びその均等範囲を包含するものとして理解されなければならない。

先ず本発明の量子暗号通信システムにおける典型的な第1の実施形態を図面を

参照して詳細に説明する。

図1は本発明による量子暗号通信システムの第1の実施形態の模式図である。図1を参照すると、本実施形態の量子暗号通信システムは、送信者の装置10、伝送路14、16及び受信者の装置12からなり、送信者の装置10は、レーザー光源1と、ビームスプリッター2と、鏡3と、光減衰器4とを備えている。

レーザー光源1から出た光は、ビームスプリッター2で参照光Lと信号光Sとに分割される。信号光Sを反射する鏡3は光の波長程度の微少な距離の移動が可能で信号光Sの位相を変化させる。

信号光Sは光減衰器4により強度が減少し、典型的な強度が光子1個程度となるようにし、量子力学的な状態変化を検出できる微弱な信号にしている。

参照光Lの典型的な強度は光子1千万個程度であり、信号光Sと参照光Lの強度は著しく異なるように調節されている。

したがって、参照光Lの光の強度が信号光Sの光の強度よりも著しく大きいため、高効率の検出が可能になるとともに、信号光Sの量子状態の測定が可能になる。

受信者の装置12は、光の波長程度の微少な距離の移動が可能な鏡5と、光の透過率と反射率が等しいビームスプリッター6と、フォトダイオード7a、7bと、増幅器及び電圧測定器8とを備えている。

受信者は鏡5を移動することにより参照光Lと信号光Sとの相対的な位相差を変化させたあと、ビームスプリッター6上で2つの光を重ね合わせる。ビームスプリッター6からの2つの出力光はフォトダイオード7a、7bによりそれぞれ電気信号に変換する。さらに、その差信号を増幅し電圧を測定する。増幅器8にはチャージセンシティブアンプを用い、その典型的な利得は30V/pC（ピコクーロン）なので、差信号に1万個の電子が含まれているときの出力電圧は50mV程度となる。

フォトダイオードとしては波長が600～900nmの光に対してはSiを、波長が1000～1500nmの光に対してはInGaAsを使用すれば量子効率90%以上、最適な場合では99%以上の量子効率を実現できる。つまり、最適な場合、参照光Lの強度が強いということから例えば1万個の光子を9900

個以上の電子に変換し、その電子数を十分なS/N比で測定することが可能である。

次に受信者の信号処理について説明する。以下の説明では簡単のためフォトダイオードの量子効率を100%とし、また増幅器の雑音は無視できるとした。

図1を参照して、信号光Sと参照光Lはビームスプリッター2で分割された後、別の経路を通りビームスプリッター6上で重なり合うので、2つの経路の光路差により干渉を起こす。

ただし、2つの光の強度が著しく異なるので干渉稿の明瞭度は低い。

図2は信号光の量子状態の揺らぎを考慮しない場合の受信者側の測定信号の模式図であり、(a)は参照光と信号光の経路の相対的な光路差とフォトダイオードに入射する光子数との関係図であり、挿入図は光路差がゼロ付近の拡大図である。図2(b)は参照光と信号光との差信号を示す図である。

図2(a)に示すように、ビームスプリッター6は信号光Sがないときに参照光Lを1対1に分割するよう調整するので、2つのフォトダイオード7a, 7bに入射する光子数は共に参照光Lの光子数 n_0 の半分程度である。それを中心として2つの経路の相対的な光路差に応じて微少な干渉稿が現れる。干渉稿の強弱は2つのフォトダイオード7a, 7bで逆位相なので、両者の差信号をとると、図2(b)に示すように干渉稿の部分のみを取り出すことができる。このとき干渉稿の振幅は信号光Sの光子数 n_1 と参照光Lの光子数 n_0 の積の平方根の2倍、すなわち $2\sqrt{n_1}\sqrt{n_0}$ である。なお、信号光Sと参照光Lの振幅は強度の平方根、つまり $\sqrt{n_1}$ と $\sqrt{n_0}$ であり、フォトダイオード7aとフォトダイオード7bとの差の最大値は

$$\{(\sqrt{n_1} + \sqrt{n_0})^2 / 2 - (\sqrt{n_1} - \sqrt{n_0})^2 / 2\} = 2\sqrt{n_1}\sqrt{n_0}$$
となる。

さらに上述したのは多数回の平均値であり、1回ごとの差信号の測定結果には信号光Sの量子揺らぎにより標準偏差 $\sqrt{n_0}$ の揺らぎが存在する。

図3は信号光の量子状態の揺らぎを考慮した場合の受信者側の測定信号の模式図であり、(a)は光路差が0度の場合、(b)は光路差が90度($\lambda/4$)の場合、(c)は光路差が180度($\lambda/2$)の場合、(d)は光路差が270度

($3\lambda/4$) の場合であり、それぞれ横軸は差信号の大きさを示し、縦軸はその信号が検出される確率を示す。

なお λ は光の波長を示し、横軸は差信号を $2\sqrt{n_0}$ で割って規格化してある。

図3(a)に示すように、信号光Sと参照光Lとの相対的な光路差が0度の場合、信号光Sが平均光子数1のコヒーレント状態の場合に得られる差信号の頻度分布は平均値が1で、標準偏差が0.5のガウス分布となる。図3の(b)～(d)の場合は、平均値がそれぞれ0, -1, 0となる。

したがって、量子暗号を実行するためには、受信者は1回ごとの測定について光路差が0度であったのか、あるいは180度であったのかを差信号の測定結果から判断することが可能になる。つまり、図3の(a)と(c)とを区別すればよいので、しきい値 X_- 、 X_+ を定めて、差信号が X_+ 以上であれば0度、 X_- 以下であれば180度と判断することができる。

このように、 X_- と X_+ とを設定することにより実効的な検出効率と誤り率を自由に設定できる。例えば図3の $n_1 = 1$ の場合に、 $X_- = X_+ = 0$ とすると、光路差が0度のときに0度と判断する確率(実効的な検出確率)は、ガウス分布を{(平均値) - (標準偏差の2倍)}から無限大まで積分すればよいので、97.7%となる。逆に、光路差が180度であるのに0度と判断してしまう確率(誤り率)はガウス分布を{(平均値) + (標準偏差の2倍)}から無限大まで積分したものなので2.28%となる。また $X_- = -0.5$ 、 $X_+ = 0.5$ とすると、同様の計算により実効的な検出確率が84.1%まで低下するが、誤り率が0.13%と非常に小さくなり、従来より優れた性能が得られる。

図4は第1の実施形態の測定結果の例であり、(a)は5000回測定したときの差信号の頻度分布図で、横軸は実際の測定電圧である。(b)は(a)のような測定を30回行って得たデータから計算機トモグラフィーにより求めた信号光のウィグナー分布関数の図である。ウィグナー分布関数は信号光の量子状態の表現方法の一つであり、ウィグナー分布関数が得られたことは信号光の量子状態の測定が実際に可能であることを示している。

本実施形態の測定では5000個の光パルスに対して差信号の電圧値を測定し頻度分布を求めたものであり、図4(a)に示すように頻度分布はガウス関数に

従っている。なお、図4（a）の横軸は実際の測定電圧であるので、分布の幅を図3の場合と直接比較するには、増幅器の利得と参照光の強度を使って補正する必要がある。

このような補正をすれば、測定された分布の幅（差信号の揺らぎの大きさ）は量子揺らぎで予測される幅と一致することが確かめられる。

図4（b）は光路差を変化させながら5000回の測定を30組、計15万パルス分のデータから求めたウィグナー分布関数である。

このように本発明の第1の実施形態では、光路差を変化させながら測定を行うことにより、信号光の量子力学的な状態の測定が可能である。ウィグナー分布関数は信号光について理論上知りうる全ての情報を含んでいるので、盗聴者の存在による信号光の変化を、より簡単に見いだすことが可能になる。

次に量子暗号の手順について説明する。

図5は本発明による量子暗号の手順を示す表であり、左欄の1は送信者の位相変調、2は受信者の位相変調、3は送信者と受信者の位相変調の合計、4は受信者の測定結果、5は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、0度又は180度のとき○を、90度又は270度のとき×を受信者に通知したこと、6は受信者が+にビット1を、-にビット0を、○になった場合につき当てはめ秘密鍵としたこと、7は送信者が自分の位相変調が、0度又は90度のときはビット1を、180度又は270度のときはビット0を当てはめ秘密鍵としたことを示す。なお、ここでは簡単のため誤り率を0とする。

まず送信者は図1中の鏡3を制御することにより、0度、90度、180度及び270度の位相の変化をランダムに信号光に加える（図5の左欄1）。一方受信者は鏡5により、0度又は90度のランダムな位相変化を参照光に加える（同左欄2）。このとき合計の光路差は送信者と受信者の位相変調の差となる（同左欄3）。

さらに受信者は測定結果に対して、上述したX-、X+の設定に従い、差信号がX-以下であれば「-」を、X+以上であれば「+」を割り当てる（同左欄4）。このとき左欄3が0度のときは必ず+、180度のときは-、90度と27

0 度のときは+と-とが等確率で現れる（同左欄 4）。

次に受信者はビットが 0 か 1 であった場合について、0 度と 90 度のどちらの位相変調を加えたかを例えば公衆回線を通じて送信者に連絡する（同左欄 5）。

送信者は合計の光路差が 0 度か 180 度であったものについて、秘密鍵として採用することを受信者に連絡する。すなわち、送信者は位相変調の合計が 0 度又は 180 度のとき○を、90 度又は 270 度のとき×を受信者に通知する（同左欄 5）。

受信者は+にビット 1 を、-にビット 0 を、○となった場合につき当てはめ秘密鍵とする（同左欄 6）。

そして送信者は自分の加えた位相変調が 0 度と 90 度のものはビット 1 を、180 度と 270 度のものはビット 0 を当てはめ秘密鍵とする（同左欄 7）。

図 5 で示すように、このようにして生成された秘密鍵は送信者と受信者とで必ず一致する。

次に盗聴を知る方法を説明する。

量子的な測定は対象に必ず影響を及ぼすという原理により、第三者による盗聴の試みは伝送信号に必ず変化を与えるので、送信者と受信者ともに気づかれずに第三者がこの秘密鍵を知ることが不可能である。

具体的な信号の変化は盗聴者がどのような手段をとるかに依存する。例えば盗聴者がいったん信号光を遮って情報を読み取り、受信者に信号を再送するという手段をとった場合、盗聴者の情報の読み取りに上述した受信者と同じ測定を行うとすると、誤った位相変調のときには（送信者の位相変調との合計が 90 度や 270 度のとき）送信者の位相変調を知ることができず、受信者に正しい信号を再送することができない。

一般に互いに 90 度離れた振幅成分の両方の情報を得ることは不確定性関係により不可能であるので、盗聴者がどのような手段で情報を読み取るとしても正しい情報は得られず、必ず誤り率の増加となって現れる。すなわち、送信者と受信者の秘密鍵が一致しない。例えば盗聴者が信号光をいったん遮って再送するという手段をとった場合は、不適切な位相変調を行う確率 $1/2$ と誤った信号を再送する確率 $1/2$ を掛け合わせた確率 $1/4$ で、送信者と受信者との秘密鍵が一致

しない。

したがって、秘密鍵の一部を照らし合わせることで盗聴者の存在を検出することができる。

また信号光の一部を分離して測定して情報を部分的に得て、分離したことによる損失を増幅によって補うという盗聴手段の場合、従来の量子暗号では低い量子効率と相まって検出が困難であったが、本発明の場合ではウィグナー分布関数の変化となって現れるので受信者は直ぐ気が付くことになる。これは増幅過程が量子揺らぎの増減を必ず伴うので、図4(a)のような測定結果において分散の増減となって現れ、ウィグナー分布関数もピーク値のまわりの分布が全体的に太くなったり非対称となり、また盗聴者が確定的な情報を得た場合のみ増幅する盗聴手段をとった場合には、ピーク値をとる X_1 、 X_2 の値も変化することになるからである。

次に、本発明の第2の実施形態について説明する。

この第2の実施形態は、伝送路として1本の光ファイバーを用いることを想定しており、上述した第1の実施形態のままでは困難である長距離の量子暗号を可能にするための実装である。そのために参照光と信号光とを時間及び偏光状態で分離し、同一の経路を伝送させるようにしたものであり、受信者の信号処理や量子暗号の手順は上述した第1の実施形態と同様である。

ただし、送信者と受信者との位相変調に量子暗号の手続に加え、別に予め定めた位相変調を与えることにより、光路差の安定性の改善と量子状態のモニターのための操作を加えている。

安定性の改善は、予め定めた位相変調の場合に予測される差信号と実際に測定される差信号との比較により行う。量子状態のモニターは一様に変化する位相変調を予め定めた位相変調として与えることにより実行できる。

図6は第2の実施形態の量子暗号装置の模式図である。

図6を参照すると、第2の実施形態は、送信者側に、直線偏光のパルス光を発生するレーザー光源21と、このパルス光を2つに分割するビームスプリッター22と、一方の経路の光、これを信号光として、信号光Sの偏光を90度回転する半波長板24と、吸収媒質により信号光Sの強度を弱くする光減衰器25と、

信号光Sの位相を変化させる位相変調器26と、他方の経路の光、これを参照光Lとして、この参照光Lと信号光Sとを同一光軸上に戻す偏光ビームスプリッター23とを備え、参照光Lと信号光Sとを光ファイバー27に入射するようになっている。このとき信号光Sと参照光Lとは互いに偏光が直交しており、かつ、時間的に離れた状態となっている。なお、図6中の18, 19は鏡を示す。

光ファイバー27の出力側には光ファイバー伝送中の偏光の乱れを補正する偏光素子28が設けられている。本発明では参照光Lの強度が強いので、この参照光Lを用いて補正を行っている。

受信者側には、信号光Sと参照光Lとを分離する偏光ビームスプリッター29と、先ほどとは逆に距離的に短い経路を通し途中で位相変化を信号光Sに与える位相変調器30と、長い経路を通して参照光Lの偏光を90度回転する半波長板31と、参照光Lと信号光Sとを時間的及び偏光方向も一致させるビームスプリッター32とを備え、このビームスプリッター32からの参照光Lと信号光Sとをそれぞれフォトダイオード33a、33bにより電気信号に変化し、その差信号を増幅器及び電圧測定器35で増幅し、電圧を測定するようになっている。なお、図6中の38, 39は鏡を示す。

このような構成により、信号光Sと参照光Lとが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、2つの光の相対的な光路差の変動を小さくすることができる。

さらに相対的な光路差の変動の影響を除くために後から値の定まる位相変調と秘密鍵伝送のための位相変調とを与える。

図7はこの発明にかかる第2の実施形態に位相変調を与える手順を示す表である。

図7を参照してさらに説明すると、左欄の1は送信者の位相変調、アンダーラインのあるものは秘密鍵伝送のための位相変調、2は受信者の位相変調、3は送信者と受信者の位相変調の合計、4は受信者の測定結果、5は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、0度又は180度のとき○を、それ以外のときは合計の位相変調を受信者に通知したこと、6は受信者が+にビット1を、-にビット0を、○になった場合につき当ては

め秘密鍵としたこと、7は送信者が自分の位相変調が、0度又は90度のときはビット1を、180度又は270度のときはビット0を当てはめ秘密鍵としたことを示す。

後から定まる位相変調の場合（図7左欄5）は、差信号の平均値が予測できるので、逆に実際に測定される差信号の平均値から光路差の変動を見積もることができる。

したがって、たとえ外的な要因による相対的な光路差の変動があったとしても、その効果を打ち消すように補正することが可能になる。

さらにいろいろな位相での差信号のデータから計算機トモグラフィーにより信号光の量子状態を得ることができる。

したがって、本発明によれば、光路差の変動の補正と量子状態の測定を両方を同時に行うことが可能になる。

産業上の利用可能性

以上のように、本発明の量子暗号通信システムは伝送信号の量子力学的な状態の測定ができるとともに、実質的に高い量子効率で伝送信号の検出ができる。

したがって、本発明の量子暗号通信システムは第三者の盗聴が不可能な暗号通信システムとして極めて有用である。

請 求 の 範 囲

1. 光信号を用いる量子暗号通信において、

盗聴の操作によって生じる信号光の差信号における振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする、量子暗号通信システム。

2. 前記量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で上記参照信号と上記伝送信号とに位相差を付与し、これら2つの信号を受信側で重ね合わせて得られる相互に逆位相の関係にある2つの出力光の差を求め、上記伝送信号の量子状態の揺らぎに依存した上記出力光の差信号の頻度分布に基づいて送信側と受信側との秘密鍵を共有するとともに上記伝送信号の量子状態の揺らぎを直接測定するようにしたことを特徴とする、請求の範囲第1項に記載の量子暗号通信システム。

3. 光源からの光を伝送信号と参照信号とに分割する第1のビームスプリッターと、上記伝送信号に位相変調を与える位相変調手段と、この伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、上記参照信号に位相変調を与える位相変調手段とを備え、

上記伝送信号と参照信号とに相対的な位相差を付与後、

上記位相変調した微弱な伝送信号と上記位相変調した強度の強い参照信号とを重ね合わせ出力する第2のビームスプリッターと、この第2のビームスプリッターの2つの出力光を電気変換する第1及び第2の光電変換素子と、この第1及び第2の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

4. 前記位相変調手段が入射する光の波長程度の微小な距離を移動可能にした鏡

を含んでなることを特徴とする請求の範囲第 3 項に記載の量子暗号通信システム。

5. 前記参照信号と前記伝送信号とを時間及び偏光状態で分離して同一の経路を伝送したことを特徴とする、請求の範囲第 1 ～ 4 項のいずれかに記載の量子暗号通信システム。

6. 光源からの光を伝送信号と参照信号とに分割する第 1 のビームスプリッターと、上記伝送信号を一方の長い経路を通し偏光する第 1 の偏光素子と、この伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、この伝送信号に所定の位相変調を与える第 1 の位相変調手段と、他方の短い経路に通した強度の強い上記参照信号と上記伝送信号とを同一光軸上に戻す第 1 の偏光ビームスプリッターとを備え、

上記伝送信号と参照信号とに相対的な位相差を付与後、

受信側にて一本の光ファイバーを伝送してきた上記伝送信号及び上記参照信号を分離する第 2 の偏光ビームスプリッターと、この分離した伝送信号を一方の短い経路に通し位相変調を与える第 2 の位相変調手段と、上記分離した参照信号を他方の長い経路に通し偏光する第 2 の偏光素子とを有しており、

時間及び偏光状態が一致した上記伝送信号と上記参照信号とを重ね合わせ出力する第 2 のビームスプリッターと、この第 2 のビームスプリッターの 2 つの出力光を電気変換する第 1 及び第 2 の光電変換素子と、この第 1 及び第 2 の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

7. 前記光ファイバーの出力側に前記参照信号の偏光の乱れを補正する第 3 の偏光素子を設けたことを特徴とする、請求の範囲第 6 項に記載の量子暗号通信システム。

8. 前記差信号に正負それぞれにしきい値を設定し、このしきい値を基準にして

前記伝送信号の状態を判別することを特徴とする、請求の範囲第1～7項のいずれかに記載の量子暗号通信システム。

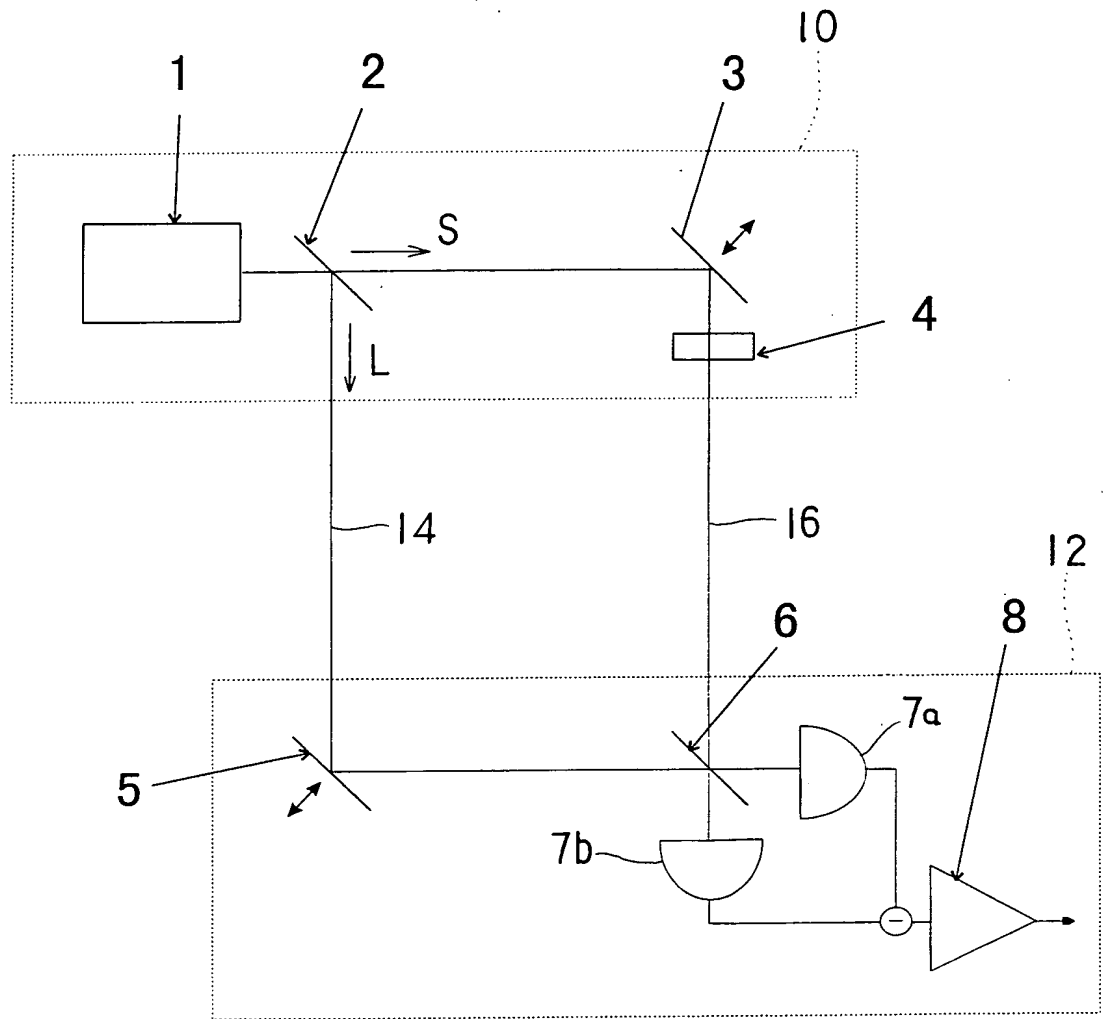
9. 前記位相差の付与を秘密鍵伝送のための位相変調の他に後から値の定まる位相変調を与えることによって、外的な要因による前記参照信号と前記伝送信号との光路差の変動を補正することを特徴とする、請求の範囲第1～8項の何れかに記載の量子暗号通信システム。
10. 前記位相差が秘密鍵伝送のための位相変調と後から値の定まる位相変調とをランダムに繰り返すことを特徴とする、請求の範囲第1～9項のいずれかに記載の量子暗号通信システム。
11. 前記差信号の誤り率の増加に基づいて盗聴を検出することを特徴とする、請求の範囲第1～10項のいずれかに記載の量子暗号通信システム。
12. 前記差信号の量子力学的な状態を示すウィグナー分布関数の変化に基づいて盗聴を検出することを特徴とする、請求の範囲第1～11項のいずれかに記載の量子暗号通信システム。
13. 前記2つの出力光をフォトダイオードで電気変換することを特徴とする、請求の範囲第1～12項の何れかに記載の量子暗号通信システム。
14. 光の波長が600nm～900nmのときシリコンフォトダイオードを用い、光の波長が1000nm～1500nmのときInGaAsフォトダイオードを用いることを特徴とする、請求の範囲第1～13項の何れかに記載の量子暗号通信システム。

要 約 書

送信者はレーザー光源（１）と光減衰器（４）とを、受信者は増幅器及び電圧測定器（８）を備え、信号光（Ｓ）を反射する鏡（３），（５）は光の波長程度の微少な距離の移動が可能で信号光（Ｓ）の位相を変化させ、信号光（Ｓ）は光減衰器（４）により強度が減少し、典型的な強度が光子１個程度となるようにし、量子力学的な状態変化を検出できる微弱な信号にしている量子暗号通信システムである。

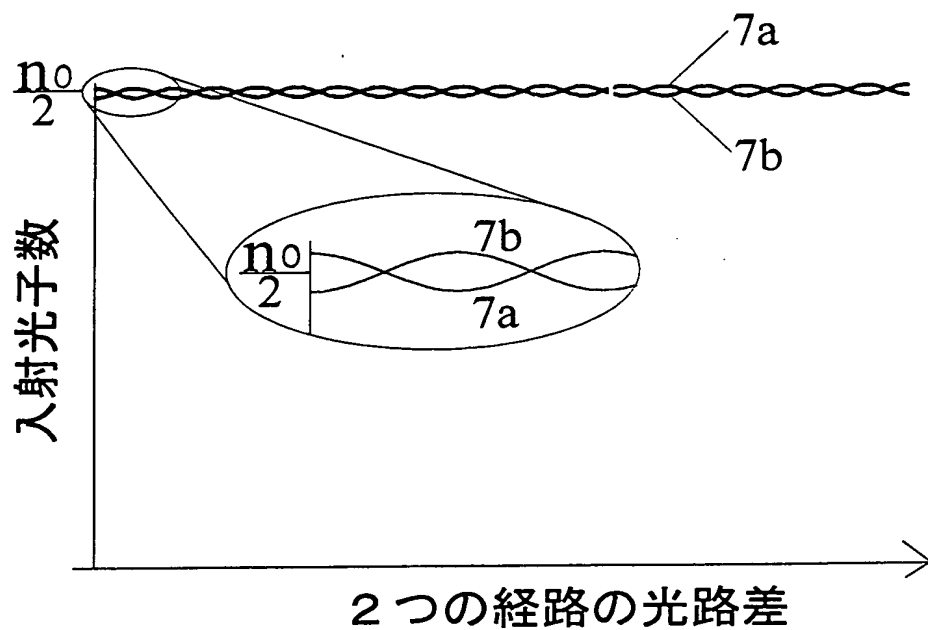
この量子暗号通信システムは第三者の盗聴が不可能な暗号通信システムとして極めて有用である。

【図 1】

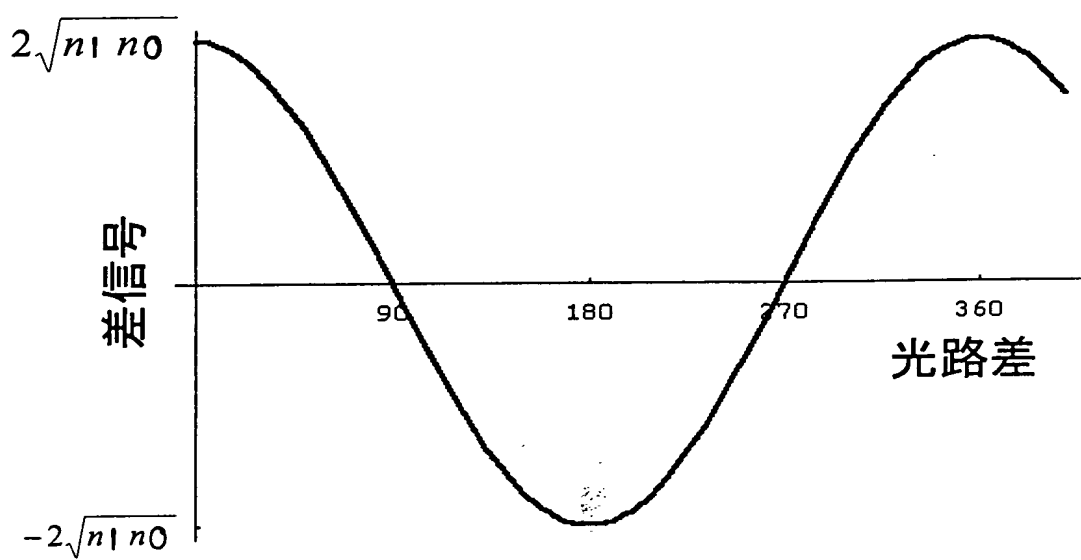


【図 2】

(a)

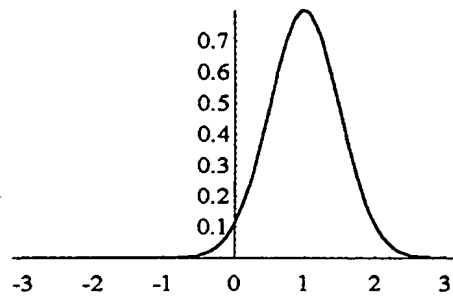


(b)

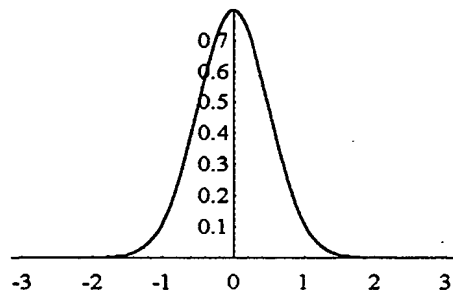


【图 3】

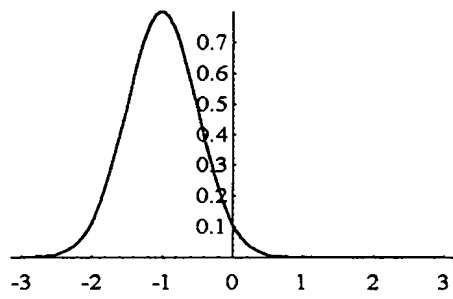
(a)



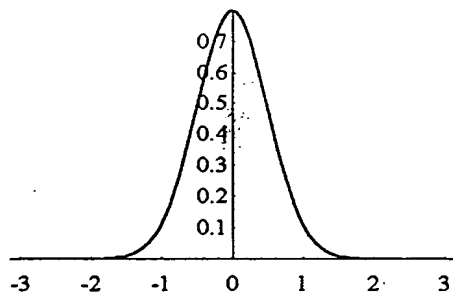
(b)



(c)

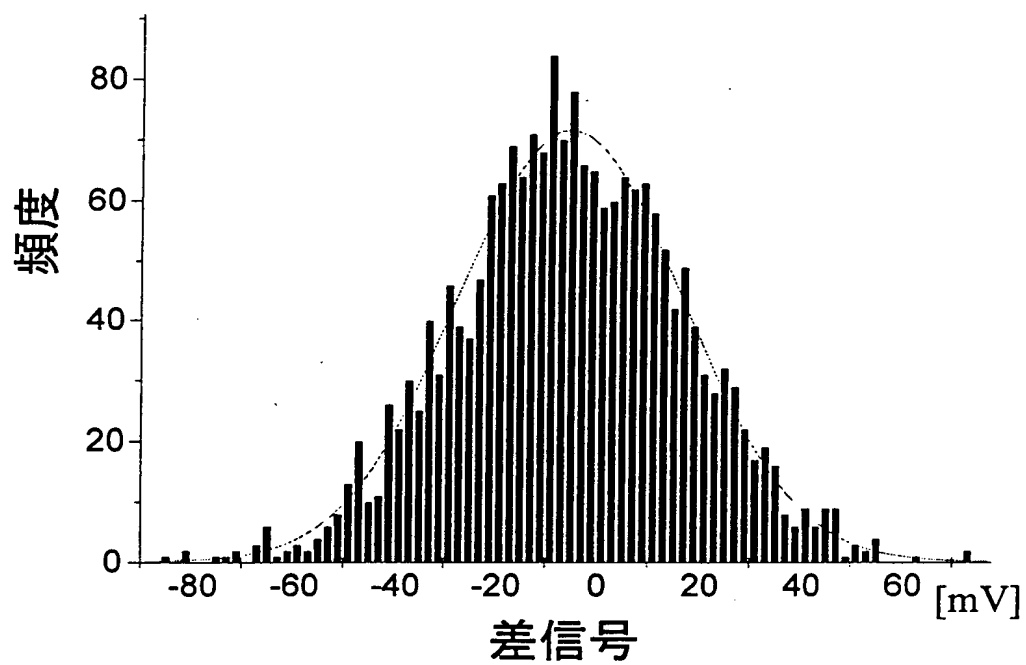


(d)

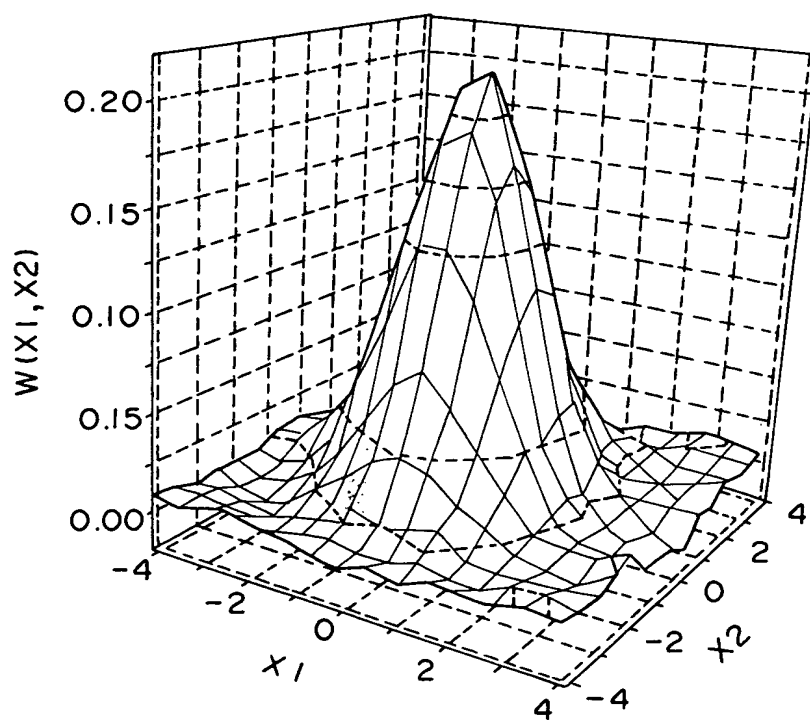


【図 4】

(a)



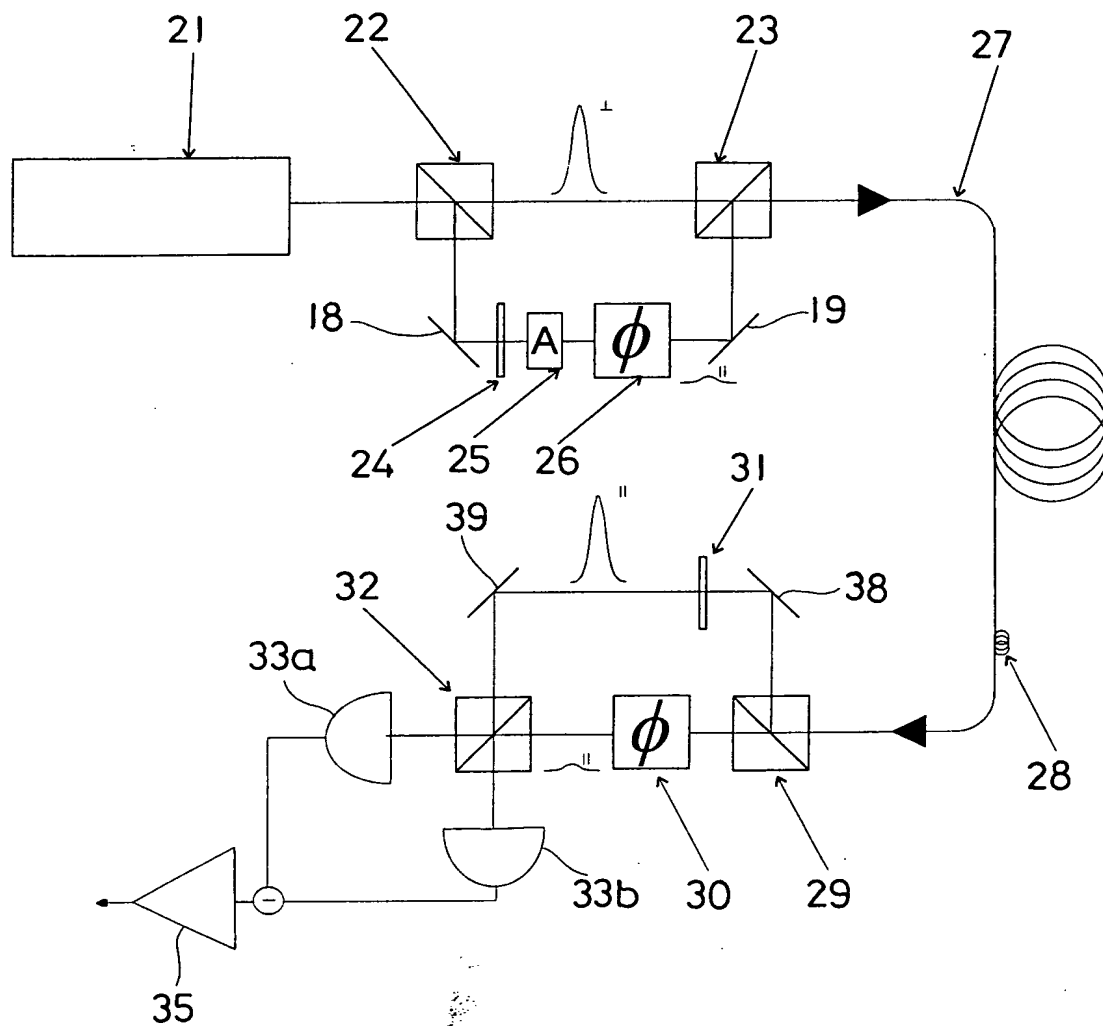
(b)



【 5 】

1	270	90	180	90	270	90	270	0	90	180	90	270
2	0	90	90	0	0	90	90	0	90	90	0	90
3	270	0	90	90	270	0	180	0	0	90	90	180
4	+	+	—	+	+	+	—	+	+	+	—	—
5	×	○	×	×	×	○	○	○	○	×	×	○
6		1				1	0	1	1			0
7		1				1	0	1	1			0

【 6 】



【☒ 7】

1	100	<u>180</u>	<u>90</u>	150	<u>90</u>	130	120	<u>90</u>	<u>180</u>	160	<u>270</u>	70
2	0	90	90	0	0	90	90	90	0	90	90	90
3	100	90	0	150	90	40	30	0	180	70	180	340
4	+	—	+	—	+	+	—	+	—	+	—	—
5	100	90	○	150	90	40	30	○	○	70	○	340
6			1					1	0		0	0
7			1					1	0		0	0

P C T

REC'D 22 NOV 1999

WIPO

PCT

国際調査報告

(法 8 条、法施行規則第40、41条)
〔PCT 18条、PCT規則43、44〕

出願人又は代理人 の書類記号 PCT001JST	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/J P 99/04328	国際出願日 (日.月.年) 10.08.99	優先日 (日.月.年) 24.09.98
出願人 (氏名又は名称) 平野 琢也		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT 18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁶ H04L9/38, H04B10/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁶ H04L9/38, H04B10/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996
 日本国公開実用新案公報 1971-1999
 日本国登録実用新案公報 1994-1999
 日本国実用新案登録公報 1996-1999

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	M. J. Werner, G. J. Milburn; "Eavesdropping using quantum-nondemolition measurements", PHYSICAL REVIEW A, Vol. 47, No. 1 (1993) p. 639-641	1, 5, 8-11
Y A		12-14 2-4, 6, 7
Y	H. Bartelt, K. -H. Brenner; "The Wigner Distribution Function An Alternate Signal Representation in Optics", ISRAEL Journal of TECHNOLOGY, Vol. 18, No. 5 (1980) p. 260-262	12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

02. 11. 99

国際調査報告の発送日

16.11.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

4229

電話番号 03-3581-1101 内線 3576

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	副島俊雄, 貝淵俊二 著; 新版・光ファイバ通信 株式会社電気通信技術ニュース社 発行, (12. 12. 1981) p. 252-253	13, 14
A	C. Marand, P. D. Townsend; "Quantum key distribution over distances as long as 30km.", Optics Letter, Vol. 20, No. 12 (1995) p. 1695-1697	1-14
A	Yi Mu, Yuliang Zheng, Yan-Xia Lin; "Multi-User Quantum Cryptography", International Symposium on Information Theory & Its Application 1994, Vol. 1 (1994) p. 245-250	1-14
A	B. A. Slutsky, R. Rao, P. -C. Run, Y. Fainman; "Security of cryptography against individual attacks", PHYSICAL REVIEW A, Vol. 57, No. 4 (1998) p. 2383-2398	1-14
A	松枝秀明; "量子暗号の現状と期待", 電子情報通信学会誌, Vol. 81, No. 3 (25. 03. 1998) p. 225-228	1-14